What is OneDrive for Business?

• 1TB of cloud storage
• Fully integrated part of Office 365 and your desktop
• Share and collaborate on work with anyone
• Intended to store personal work files – not team documents
Why use OneDrive for Business?

University data is not safe in ‘personal cloud storage’
You must move it to OneDrive for Business

Personal cloud storage
E.g.: Dropbox, Box, Google Drive & OneDrive

• Private service
• Files owned by you
• Personal account

OneDrive for Business

• University service
• Files owned by University
• University staff / student account
How to use OneDrive for Business

USE for:
• Individual:
  – storing your personal work files, when others don’t need access to them
• Ad-hoc, short-term collaboration (internal and external)

Do NOT use for:
• Permanent team or department sites (external or internal)
  – Provision for long-term team and department collaboration will be delivered later in the Collaboration project
What can you put in OneDrive for Business?

OK to store:
• Your own working files, including personal and confidential data*
• Data that you are preparing for sharing with others
• Data that you are sharing with others for short-term collaborative work

Not OK to store, if... **
• There are long term preservation requirements
• Others should have continuous access to data
• There are specific license conditions, e.g.:
  – Research funder requires data to be hosted in-house.

(*) Data Protection and Information Security policies apply
(**) If you have specialist data requirements contact the Service Desk to discuss your case
Research Data

• OneDrive for Business provides secure storage in Microsoft’s data centres (EU) certified to latest security standards:
  – Data encrypted at rest and in motion
  – University retains control of data

• **Safe** for valuable research data containing **personal** and **confidential** information

Always check your Research Funder requirements before storing your data in OneDrive for Business

For more information on Research Data Management see

http://plymouth.libguides.com/research/rdm
Keeping your data safe

• **Syncing***
  – You should only sync sensitive data to a device for short-term use
  – The device must be **encrypted, password protected** and set to lock automatically after a period of inactivity no longer than 15 minutes

• **Sharing**
  – Think carefully about **what you need to share**, particularly if sensitive
  – Consider **how you share it** and **who you share it with**
  – Do not share via link – always **require login** to access files
  – Review what you share regularly – **revoke permissions** if no longer necessary
  – **Copyright**: have you got rights to share?

(*) See Encryption policy for details or contact the Service Desk for help with encryption
Keeping your data safe and usable

• Deleting
  – Deleted files go into the OneDrive for Business recycle bin
  – They can be recovered for up to 90 days
  – Take care when deleting important data from OneDrive for Business

• Access
  – When you leave the University, files stored in your OneDrive for Business will become inaccessible and eventually deleted
  – Do not keep files permanently in your OneDrive for Business that will be required by others in your team or department